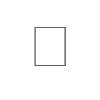
**Transcript**

August 4, 2025, 8:05AM

 **Koide, (Kayo)** started transcription

 **Koide, (Kayo)** 0:37  
Hello.

 **Ward, (Aaron Samuel)** 0:42  
Hello.

 **Koide, (Kayo)** 0:48  
The it's.

0:48  
For the CTO Mt we have the risk.  
Update so you can hear us all right.  
Yep, Yep. Good.

 **Speaker 1** 0:58  
So Quitassa's already ready to go.  
So we also have the new yens here.  
So is your.  
Oh, we used to invite yens once a month at the end of the month to talk about risk for 30 minutes.  
And I think for this one it's a good bit. Shinobu is here to help understand you with this new thing that we've got going on with the risks. I'll be quite clear this on over to you.

 **Koide, (Kayo)** 1:22  
M.  
Hi. So at the firstly, I'd like to follow up with the tasks from that from the last meeting. So at the first one at the confidentiality risk management.  
Develop a policy to manage confidentiality risks at the project level and ensure compliance.  
Any probe or something?

 **Speaker 1** 1:55  
I think I can say. Does anybody remember about this?

 **Ward, (Aaron Samuel)** 1:56  
Uh.  
Yeah. So, so I remember we discussed this. I actually don't haven't actually done anything to to move it forward. I guess I'll, I guess we already have a process in place, right, which we put in place in an ad hoc basis really for the.  
For the Um.  
For the product projects but also for the other I guess sensitive projects as they come up and we you know we we we always sort of ask and and clarify during the intake process you know what what what's appropriate for the project with with the stakeholders and and and then we you know we've got various controls in place.  
For how we report and how we how we share the information depending on what's required. But I I guess the the the question here is this is about having a policy in place. Does does this need to be like a formal a formal policy that we need to register in the policy house somewhere or or or or or?  
Register the rule or or what? What's what's actually needed here?

3:03  
Can I ask one question because?

 **Speaker 2** 3:06  
Take a step back. I thought we were supposed to look at the the risks and we we consider it if these are still the highest risk.

 **Speaker 1** 3:14  
Yeah. So then yeah, so today.  
So we're looking at the the risk for ACF, right?

3:17  
Friend.

 **Speaker 1** 3:18  
And we use this as a brainstorm.  
Recessions, right when I say OK for each of us.  
She's got a.  
On this.  
What keeps you up at night for this risk?  
Wait, wait, wait.  
And that's what we did last time, right?  
Right. And last time we did a we had a the chat box come very hopefully about what we did and then there was some follow up questions there.

 **Koide, (Kayo)** 3:32  
I.

 **Speaker 1** 3:35  
So you can see like IT risk confidentiality risk and then they came up with some suggested actions, which is what kurtisan's reviewing now, right. Right. Right. So for me, I mean I find I mean.  
We probably all forgot about this.  
We did it once and that's it.

 **Koide, (Kayo)** 3:48  
Oh, so name.

3:49  
The second part.

 **Speaker 1** 3:50  
So yeah, I think for maybe for just for that first one.  
You know, it's up to us if we need a policy or not, or if there's already an existing.  
How's it guys?  
We already do a risk review on all our projects.  
It's actually part of every document, right, Aaron?  
I mean, it's already in there, right?  
You you go in, they fill out an excel sheet and they get it. Based on this, it's a level of high minimum.

 **Ward, (Aaron Samuel)** 4:13  
So, so I mean, I mean to me and and maybe this is the chat bot or my memory is not not not functioning but but this, this, this, this, this, this, this is more about the sensitivity within the sensitive information, isn't it?

4:16  
Yeah.

 **Ward, (Aaron Samuel)** 4:30  
And and and how we and how we manage that and that's not necessarily listed in the project risks today, but it's more we we more we handle it from a process point of view at the intake process. If it sounds like this is something that's confidential, we ask the questions.

 **Koide, (Kayo)** 4:30  
Mm.  
Yes.

 **Ward, (Aaron Samuel)** 4:50  
And the take and then and based on that you know we we we have in our processes we we we we have controls in place like who can see the the reporting on this what what information we we we we publish. So we agree on what's required upfront and and and then.  
You know, through access control and various other things. When we onboard the PM and onboard the team, we we put the the controls in place. But this is not, this is not documented any anywhere actually.

5:24  
OK.

 **Speaker 1** 5:24  
So then you can see this confidentiality concerns.

5:27  
Aaron highlighted.

 **Speaker 1** 5:28  
That's what was picked up for that action.  
All right, so this is based on the conversation we had.

 **Ward, (Aaron Samuel)** 5:38  
I mean my, my, my, my view, my, my view, what we're doing at the moment works and it's not it's not one-size-fits-all here either, right? Because there's there's there's there's different levels of concerns on confidentiality based on the.

 **Speaker 1** 5:39  
So I guess for now it hasn't changed, right?

 **Ward, (Aaron Samuel)** 5:57  
On each project.

6:00  
OK.

 **Speaker 1** 6:01  
So maybe query? So I'm just trying to think what's the best way to do this right? This is only the second time we did it.  
Maybe we just start at the top and we work our way through.  
You know the each one and we say, do we still agree that this is a risk?  
Has anything changed since you did this? What, two months ago?

 **Koide, (Kayo)** 6:15  
Mhm.

 **Speaker 1** 6:16  
The main point here is so that I wanted to this quarterly. I think risk wants to do it monthly.

 **Koide, (Kayo)** 6:19  
Stop.

 **Speaker 1** 6:22  
Monthly is probably too much.  
Quarterly is for me to also because most of the time I run my ACF reports.  
Based on what I feel the discussions I have with you on 101 and this is more to sort of flesh out the risks I see from my butchers to say, have you thought about this?  
Have you thought about that?  
And that helps me write a more.  
Better PCF report based on my underst.  
Anding. So for now I think maybe we start at the the top and we just work our way through.  
I mean, did brisk have a?

 **Koide, (Kayo)** 6:56  
Means the top means this one. Sorry, top means here or follow up task. OK, OK, confidentiality.

6:56  
Suggestion.  
Side yeah.

 **Speaker 1** 7:01  
Yeah, like confidentiality risk.  
Pull up task for now is I think scrapped because I don't think anybody's followed up with anything and I think I would rather, you know, we actually do distribute well.

 **Koide, (Kayo)** 7:08  
OK, OK, right. OK. I'm actually I shared this. I shared this this two months ago to all M.

 **Speaker 2** 7:14  
We can technically say some of these are fixed, right? Like.

 **Speaker 1** 7:22  
Yeah, exactly 2 months ago. And I don't think anybody's looked at since then.

7:24  
But.

 **Koide, (Kayo)** 7:24  
Are you OK? OK, OK.

7:26  
I got me.

 **Speaker 2** 7:27  
I was pragmatic. I wasn't theirs.  
I did read it once, OK.

 **Speaker 1** 7:30  
Has anybody looked at this since then?  
OK. Like when when this is a new process, right?  
We're trying to learn, right?  
So it is what it is I'm trying to be pragmatic here.  
I want to get value out of this conversation.  
So for me it's more about OK.  
Do we still two weeks, two months ago, we came as a Guinea pig for Herman to do this, I thought at the time we definitely seem to get value out of it.  
There was a good discussion. We actually spent the whole 40 minutes and as you can see, quite a lot of content came out of that.  
I think it and it helped me for the Q2 ECF report.  
I use that those thoughts in the Q2 ECF report.  
I think now it's more about going through this again and do we think since two months ago has anything changed?  
Do we think the the risk around confidentiality has decreased given some of the stuff that has been released? You know, in June there was all the cipher craft went live?

8:24  
Yeah. SPC mail.

 **Speaker 1** 8:26  
I get some of you send stuff, I get emails now and I get annoying when I send that e-mail remotely.  
I think the risk has dropped.

 **Speaker 2** 8:35  
Yes, it's under more.  
Well, it's more visible for sure.

 **Speaker 1** 8:38  
So in terms of looking at this.

 **Speaker 2** 8:42  
You can technically say that we still use other systems like Box, but that's another system that we use.

8:43  
Of course.

 **Ward, (Aaron Samuel)** 8:45  
Great.

 **Speaker 2** 8:50  
But again for file transfers.  
But if it's a, you know e-mail file transfer, even the you know the FSA says stop using PPAP, which we don't do anymore.  
Yeah. And we use this.  
So yes, in that sense for automated DLP I could say you can definitely say that we can't to another level maturity wise.  
Yeah. And say that it's something that is under control for sure.  
At least to a certain extent.  
But if we start talking about that Microsoft purview, that's another story.

 **Ward, (Aaron Samuel)** 9:13  
Oh.

 **Speaker 2** 9:17  
Yeah, because that's about information classification, which we still don't have it completely under control, yeah.

 **Ward, (Aaron Samuel)** 9:25  
So I mean, I mean I've stopped since the DL PS in place. I've stopped people from sending stuff out outside, which maybe I wouldn't have necessarily picked up before. So and it's been quite quite good to just remind people what they can and can't do.

9:25  
OK.  
OK.

 **Speaker 1** 9:46  
So then I guess Kui Nissan. I mean, are you going to look at the transcript later on to write the notes or. Yeah. OK. So we don't need to do this. OK.  
So then the confidentiality concerns around.  
Yeah. As I said, it's the across the different categories, Aaron.  
So we see there's one for the specific projects, OK? You think there's still a thing there?  
We need to look into that.  
Data governance so that your son so.  
You can see that Michael pointed out.  
Challenges in the past.  
Building data dictionaries clean up necessary data, improving data governance, spread authorized data sharing.  
So I think we had, we actually had a session since then with Calibra.

10:33  
Yeah, we have another session is.  
Thank you.  
Last week and we decide to start training.  
Yeah.

 **Speaker 3** 10:43  
Inside of DMA and I think.  
In this month, we will.  
To complete \*\*\*\*. Yeah. And then I would initiate the POC inside of the MA and to understand how to use the software and also the plan, the integration.  
With our system and as well as the the detailed governance crown will be decided after that and as we can.  
And conduct a certain part of the data governance inside of our division. And I think that we can start to load it out to the company wide.

 **Speaker 1** 11:28  
Yeah. So deliver is A is a group tool that's used for data governance and data mapping.  
It's actually, I think, something that.  
I think we really need the presentation that they gave to us, the group team.  
It's a lot of work to get it up and running, but then it basically maps.

11:44  
Data.

 **Speaker 1** 11:45  
Company where it all is.  
It's it's pretty spectacular software actually, but it's gonna take time to implement, right?

 **Speaker 3** 11:53  
Yeah. Yeah. And yeah, I will want to have a quick win, but today is still won't have a whole company training to us. So I shortened it.  
But they yeah.  
So yeah, you you have to take 8 hours to have the training.  
So so.

12:10  
Yeah.

 **Speaker 3** 12:10  
We will do that. Yeah. OK.

 **Speaker 1** 12:12  
So that should help with some the data governance data visibility, right?  
So OK automated DOP. We talked about new product information.  
So to me, Sam, we have 1000 people in this company and 500 of them have signed an NDA on product development.  
So thumbs up for that, yeah.

 **Tsutsumi, (Hideaki)** 12:28  
Paul, Paul, Paul Hobbit.

 **Speaker 1** 12:32  
So how many 400. OK.  
That's better. OK, so.  
Is there anything you has anything changed here or?

 **Tsutsumi, (Hideaki)** 12:37  
Uh.

12:38  
Evening.

 **Tsutsumi, (Hideaki)** 12:39  
Yeah, for this, maybe I just as you know, it has been discussed that the project board and also the product board, a new NDA rule is set. So based on the new rule, our country under refresh in the

12:48  
Yeah.

 **Tsutsumi, (Hideaki)** 12:56  
Process and also the digitalized process. Application process is ongoing, ongoing with support from the. It will be. It will be.  
He used from the next new project big one.

13:20  
OK.  
OK.

 **Speaker 1** 13:22  
So it's trying to get some a little bit more control around that, correct?  
So then from the next big project.

 **Tsutsumi, (Hideaki)** 13:26  
Yeah, yes, yes, yes, yes, yes, yeah, yeah, yeah.

 **Speaker 1** 13:29  
Will really limit who has access to it and will have records of who's got the NDA.

 **Tsutsumi, (Hideaki)** 13:33  
Yeah, clarify the rule, process and the ownership. Uh and the process. Uh, it's a clear, uh, clearly clarified.

13:43  
OK.

 **Speaker 1** 13:46  
Sounds like we've got a few things moving since the last two months on this, right?  
So what's the thing you should mention about like DOP solution?

13:52  
You bring in the dead, that's also likely helping you to prevent.  
Yeah, exactly.

 **Speaker 1** 13:57  
And I think the the only other one that you're made automated DLP is Michael has been contacting.  
The group on purview and yeah, so that that, that discussion is ongoing.

 **Speaker 2** 14:09  
Ross has been.

 **Speaker 1** 14:10  
Yeah. Ross has been pushing.

 **Speaker 2** 14:11  
So one of the biggest changes is like we we actually when you remember for right now for I don't think we rolled it out for all the employees yet this week but.  
The emails and everything on your word docs. You know, for information we said, OK standard is you know exactly fault is internal. OK now from there we have to make sure that people start using it, making sure it's confidential and making their sure that they choose the correct.  
No, it's not.  
You know, rolled out for everyone yet and it takes training and of course then it's more of culture again.  
So it's gonna take some time to build that, of course. But we did go through the first step.  
We can do it now and it, well, I don't know about Guru, but again Japan has started again.

 **Speaker 1** 14:50  
Yeah, as the first.

 **Speaker 2** 14:50  
Person first you know BU to start.

 **Speaker 1** 14:52  
Yeah. 2 litre trendsetter. Yeah. OK, good.

 **Speaker 2** 14:56  
So and yeah, as you said for the DLP part, I think the EC last time the ECFI think the DLP part was one of the things where we said we're a little bit lower that we need.  
So you can actually for the next ECF we can say yeah, we've improved and you can just bump it up.

 **Speaker 1** 15:09  
Yeah, that was the argument I had in the ACF review meeting was yes, we've implement, but we talk about P2, we're still high.  
Yeah. And I think as we go through Q3, by the time we get to.

15:19  
End.

 **Speaker 1** 15:19  
Of Q3, I think we'll be in a better position to maybe think about going back down to medium. That was the argument I had previous, OK.  
Anything else on this one? Confidential, no.  
No. OK. Operational change risk.

15:36  
Aaron.

 **Speaker 1** 15:39  
Better defined processes for operational change include prioritization, communication, Michael added. The FSA guidance points of updating process definitions.

 **Ward, (Aaron Samuel)** 15:47  
Yeah. So I guess, I guess this is going on on on ongoing. So discussions around around this have kicked off and Koide-san and and and Yasim Otosan are leading it working with I think Fujino-san and and the other PMS as well to to talk about these things incorporate some of.  
The things that Fujino Sun's been been been been been working on. So this, this, this is ongoing. This is part of the continuous improvement and continuous systematic improvement goal for for for for for for this year I think in the last.  
A couple of weeks. There's also been some discussions with the with with Chris and and and his team about you know the the the ARB part of the part of the process and how how we improve the engagement with.  
With architecture through through the process to make it go go smoother. So this is on on ongoing work.

 **Speaker 1** 16:51  
OK, racial changes.  
Plan mentioned CS pipeline will manage.  
How we yeah, some projects as well to collect exemption from these processes.

 **Vizzini, (Alain)** 17:05  
Yeah, so we we.

17:05  
I think we.

 **Speaker 1** 17:06  
I think we whacked the live J ones on the head, right. We fixed that.

 **Vizzini, (Alain)** 17:09  
Yeah, correct. So that that's what we did. We worked out the communication with Chris, work together on that, making sure everybody knows. So we reinforce the rules at town halls in standards. We updated the the company policy, make sure it's known and we reminded people that.

17:23  
Yes.

 **Vizzini, (Alain)** 17:27  
Even though it's written in policies and they most likely don't read it, they should know it and there's no excuse. And the ARB is the point where they have to go and if they say no, it's no. So since then there was a significant improvement I heard, but we we we keep vigilant.

17:39  
Yeah.

 **Speaker 1** 17:47  
Yeah, we still need to monitor yourself the same as going to the cab.  
Right. Change advise report.

 **Vizzini, (Alain)** 17:51  
Yeah, same, same, same, same, same, same. Look at no change.

17:53  
Yeah. OK.  
No exceptions.  
Yeah. Perfect.  
OK.

 **Speaker 1** 17:59  
That's pretty good FC guidance.  
Yeah, I mean the only one here in the FSA guidance of infra operational changes.  
Now we've got that new.

18:12  
Yeah, yeah, yeah.

 **Speaker 2** 18:13  
About that actually just today that one talk to you this morning.

18:15  
The.

 **Speaker 2** 18:17  
Yes. So around Salesforce with.  
Our system mate my page.

18:24  
My page.

 **Speaker 2** 18:25  
Yeah, my page and and in link. Yeah, yeah, yeah. So actually on that part, just just additional notes for FY for everyone.  
Yeah, I. So it's acoc, right? Yeah.  
The COC committee.  
Yes. So that one, Shinobu is actually talking to enosan.

 **Speaker 4** 18:40  
And my thing in link.

 **Speaker 2** 18:40  
Already OK.  
Yeah. So from the business perspective, I've been doing it on the ID side.  
So we'll see like.

 **Speaker 4** 18:50  
Two, like a streamline there, like the ones coming from a more compliant side directly. And I get to perform a bit of like a high level Japan analysis. And one of the topic was about this like.  
This is used for the user accounts for those customers information, whatever, and then that's where it into like what can receive, which is like more like asking for the technical details.

19:09  
You know.  
Yeah.

 **Speaker 4** 19:12  
So I tried to kind of share that information.  
So, like if we don't have two different stories, those need to be well aligned because like it should really go to like FSA already.

19:26  
Show it.

 **Speaker 4** 19:26  
No, not not.

 **Speaker 2** 19:27  
That's that's for that, because they have the CLC. Yeah, right.

 **Speaker 4** 19:30  
Yeah, like a doors should be like a very much early.  
So like again, we need to handle like 1 streamlined.

19:37  
Yo.

 **Speaker 1** 19:37  
Because we're also doing the subsecurity self-assessment.  
Yeah, it's gonna be sent to the FSA in two weeks time.  
Yeah. And we need that to be consistent.

19:45  
Exactly.

 **Speaker 1** 19:48  
So this is this is this one about this one. There was new requests came in last Monday about, you know obviously lots of customer information's being shared recently and hacked and the stuff. So they want to make sure there's MFA and you know we're we're reviewing when.  
Customer logs in, so monitoring if there's any suspicious activity when a customer logs in or logs out, or transactions that are suspicious, they want us to actually start to try to manage that.

20:14  
Yes.

 **Speaker 1** 20:16  
That's definitely a risk, but I think it seems to be handling it OK and it's gonna be.

 **Speaker 2** 20:22  
Well, it's just for now, but we do already know right now we don't have even mfe enabled.

20:28  
Yeah, yeah.

 **Speaker 2** 20:29  
So that means right now it's just from the from the FSA, which means it's not required, right? But.  
As I said at the IT town hall, that's what probably happened back in February for all the security industry.  
Yeah, that means they all put it in.  
Because when it's AUC from the, that's literally saying do it, yeah.  
And that's what we probably have to do this time around because they're saying for the full financial independ please do it, which includes us now.

20:59  
So we.

 **Speaker 2** 20:59  
I mean, we might not have it now, but we need to make sure we have a scheduled plan to say, OK, what kind of MFA is it going to be?  
Pass keys or whatever, but if we're only using IDs and passwords, which is the current situation, do need to up it up a little bit, yeah, but that's something that we need to make sure that we do. But the business also understands that and I think that part.  
I will be talking to -1 such a good stuff, so it'll sound.  
They know what we're talking about. OK? But we also have to push it. Not just, but from NN perspective. We have to push.

21:27  
It yeah, yeah. OK.  
OK.

 **Speaker 1** 21:30  
So this is a changing regulatory environment.  
New things happening then they're coming out. So we need to be able to adjust this. So it sounds like from here, from a point of view of risk around FSA guidance and operational change, it sounds like we've got a pretty good intake process where we're aware of the.  
Stuff that's coming in, it's gonna probably take a year or two to sort the technicals out as per usual, but at least we have that process of visibility on these new things.

21:51  
Yeah.

 **Speaker 4** 21:59  
This is like additional information was like.  
This is like triggered by the more security houses, yes. So those are the area they first focus on.  
Yeah, like the insurance company will be like the second third tier. That's what you say.  
However, we don't want to be the last runner, and in the meanwhile.

22:15  
No.

 **Speaker 4** 22:18  
That's in no Sound's team has been conducting other insurance company.  
What are the measures they are in place, so maybe that you can also like to reach out to those people.  
That that the resort of the survey, how other competitors are doing it is about the current measures in place and what is a direction going forward.  
Yeah. So I think that that's might be also good.  
So I can like chat with them and then that's.

 **Speaker 2** 22:43  
Well, let's talk for sure.

22:45  
The yeah.

 **Speaker 2** 22:46  
And then we'll decide.

 **Speaker 1** 22:48  
To see that giving out 65 year old corporate owned life insurance SMEs that you.

22:53  
Know.  
OK.

 **Speaker 1** 22:54  
And paying a smile phone that they don't have.

22:57  
Exactly. Exactly.  
OK.

 **Speaker 1** 23:00  
Good updating manuals at the.  
Updating process manuals, yeah, updating documentation.  
Yeah, I mean, this is this is correct.  
Plus R23R24.  
R-25 Auto ready processes.  
You should be updating your manuals regularly, and I think most of you are. From what I see. So.

23:20  
OK.

 **Speaker 1** 23:20  
That's good. IT risk.  
Risk risk management inspections, OK.  
So yeah, we're actually with offshore inspections.

23:31  
Nice guys.

 **Speaker 1** 23:32  
4 of you in this call are going to be in Vietnam next week.  
Doing it tomorrow, tomorrow.

 **Vizzini, (Alain)** 23:37  
Tomorrow.

 **Koide, (Kayo)** 23:38  
Tomorrow.

 **Speaker 2** 23:40  
Hey, at least we're all not on the same plane.

 **Ward, (Aaron Samuel)** 23:41  
Hmm.

 **Speaker 2** 23:44  
That's a good.

 **Ward, (Aaron Samuel)** 23:45  
Mhm.

 **Speaker 1** 23:46  
Thing. Yeah. Hiroshi and I will hit the Fort down here and try not to break the place while you're away. And please don't break Vietnam.  
You're there with Pierre?  
He's got a reputation so.

 **Ward, (Aaron Samuel)** 23:56  
OK.

 **Speaker 1** 23:57  
Here you go. So that's good.  
I'll show inspections.  
I think one thing on top of this, we did the inspection of our core vendor DXC in.

 **Ward, (Aaron Samuel)** 24:08  
Kobashi.

24:08  
Chichong Cha Cha Chong Chong.

 **Vizzini, (Alain)** 24:09  
QB.

 **Speaker 1** 24:12  
But that also found some stuff that is a little bit.

 **Ward, (Aaron Samuel)** 24:16  
It.

 **Speaker 1** 24:17  
What's the right word?

 **Vizzini, (Alain)** 24:17  
Concerning.

 **Speaker 1** 24:21  
To improve. So I think that this is good, that we've actually started, restarted that conversation.  
Hopefully I'll get a report by the end of August and we'll see what we need to do.  
But that's good ransomware risk, OK?

 **Koide, (Kayo)** 24:36  
H.

 **Speaker 1** 24:36  
We still need to make sure everybody does their hoxhut training please because.

 **Vizzini, (Alain)** 24:39  
Yeah, Matusch came to my town hall last week, Thursday and Wednesday, and reminded people about that, reminding them about the risk of oversharing information on public sites and social networks.  
It's to avoid having I curls map too clearly who's working with who in which company. So yeah, I did a good job showing that. Kudos to Matus.

25:02  
Yep.

 **Speaker 1** 25:06  
Yeah, cool. OK, good stuff, right?  
Yes, I got.  
I got one the other day I'm at work.  
My work e-mail and then one of my personal e-mail.  
Sent a Ministry of Justice. My my number had been used very things that I need to contact him. Otherwise they kick me out of the country on my work e-mail and my personal e-mail.

25:24  
About where they take it.

 **Speaker 2** 25:29  
So, he argued, it argued.

25:32  
For sure.  
Ridiculous anyway.

 **Speaker 1** 25:37  
Way too many things I'll say, right?

25:42  
I was.  
I don't want to be kicked out.

 **Speaker 1** 25:43  
Of the country. Yeah, go ahead.

25:47  
Legacy systems.

 **Speaker 1** 25:49  
Yay, we've done a lot in the last two months.  
RFP is up and running. Luna is good.

25:55  
That's positive.

 **Speaker 1** 25:55  
The risk is still there, like we've only just started. The risk has not changed.  
We still have a lot of problems with legacy, but at least we're sure we're starting on the path towards getting that done so.  
I'm actually feeling a much better place than we were two months ago.  
About that I'm asking.  
Alain.

26:13  
And you try.

 **Speaker 1** 26:13  
Were thinking about this last time.

 **Vizzini, (Alain)** 26:13  
Still continuing, there's not much we can do. We have the CHM 02 control that says that we don't do, we don't use non production data in non production environments. Maybe we do that test a bit too often, but at least it's here.

26:27  
Yeah.

 **Vizzini, (Alain)** 26:30  
And we are reviewing it and I hope with Suzuki sound we work on putting the right level of priority on this test.

26:31  
Yeah.

 **Vizzini, (Alain)** 26:39  
Yeah, see, it's still ongoing, so only.

26:39  
OK.

 **Speaker 1** 26:43  
Any other issues with legacy?  
I mean, I think we're in a very good place with the Oracle.  
Article on the the laptops on our things right, getting it out of yeah.

 **Vizzini, (Alain)** 26:54  
Oracle Java, Oracle Java. It's more than a legacy. It's a it's a vendor thing because Java itself, even if you use the latest Java 21, it's you still have to get out of it. But next year, from next year it will become that because the next phase.

 **Speaker 1** 27:08  
It's not fair. OK. So then we'll.

27:11  
Yep.

 **Vizzini, (Alain)** 27:12  
Will be to exit Java 1 Java 8 because the version we will be using will be out of end of life in November 2026. So we have one year to extract to exit Java 8 which is or at least could be called a platform or legacy system.

27:22  
OK.

 **Speaker 1** 27:30  
That is the system risk, yeah.

 **Vizzini, (Alain)** 27:33  
Risk.

27:34  
How much? What?

 **Speaker 1** 27:35  
What's on Java?  
Is it only the Nomura Excel tool or is it a TRIA is on?

 **Vizzini, (Alain)** 27:37  
No, no, no, no, no. We have ACS which is the tool with the green screen. The terminal emulator we use for Java which is using one Java, sorry for Live J which is in Java 1.8. We have Atria which is using it.  
And there is one other vendor tool. The name eludes me, but it's in the minutes of the the the meeting of this week, so yeah.

28:04  
Yeah.  
OK.

 **Speaker 1** 28:05  
That's definitely a risk. I mean, that's something that's a big systems there, so.

28:09  
Ya tudi gajra.

 **Speaker 1** 28:10  
A tree or like we really need them to start working on that now, right?  
Yeah, you know, we'll find a better next year.

 **Vizzini, (Alain)** 28:15  
I told them already.

 **Speaker 1** 28:17  
How did Dan Osun react?

 **Vizzini, (Alain)** 28:20  
I told his team they were in the meeting. Yeah, but should we wait for you to get a project and money to look at that? I say no, man, just stop doing that. Just stop now. You know, for years you have to do it. Just do it now. Stop.

28:28  
Start right now.  
OK.  
OK.

 **Speaker 1** 28:40  
Good technology innovation.  
Yes, I think managing the risks associated with shadow IT.  
Luckily, thank you for the you know.  
ECS EUD as we thought we only had 599 apparently last week I logic did the presentation in the town hall and I said 599, put it on the screen, said we're going to work it out coal then reminded.  
Ken over the drink session on Wednesday.  
Afternoon. That actually is a bunch of logic apps there and there's 800 logic apps.  
And some of them may or may not be in the list that we have for EUC. Zeds. Yes. So that 599 could potentially be 1400.

 **Speaker 2** 29:32  
Well, I mean, there are some of them inside the current 500.  
Yeah, but obviously the numbers are not matching.  
So that means yes, we're missing some.  
So it will definitely go up. Yeah, but it is also the way we got that number.  
We requested all of our DMS. If you have any UCS or UDATES based on yes and then say, hey, put them in.  
Obviously some people thought logic apps was included.  
They put it in.  
Some people did not.  
And that's why we have a different gap.  
So there's an explanation of why we have missing, but it's also oh good reminder that, yeah, maybe it's good to check from the back end too, to see how many we have already. OK.

29:58  
What's up?  
Yeah.

 **Speaker 1** 30:06  
So go to San's report that he's a very nice report.  
We need to update that with this additional.

 **Speaker 2** 30:12  
Yes. So we do have to check with, but then of course that we.  
Don't have access to this.  
We have to ask call for help on that.  
So they did.  
So they're in the going to have a talk saying what kind of this and then get the list for both and then they're just gonna do some checking and see, OK.  
How many are we missing right now?  
Yeah. Then we should get some notes.

30:30  
OK, OK.

 **Speaker 1** 30:31  
So that's Cole in the.

30:35  
EA area.

 **Speaker 1** 30:35  
Right. The architect for cloud systems.  
So we need to make sure that we get this information.

 **Ward, (Aaron Samuel)** 30:42  
I.

30:43  
OK.

 **Speaker 1** 30:45  
Innovation, I think.  
Apart from that, we're doing some pretty good stuff with regentic. I think you're working on that stuff, so.

30:55  
Yeah.

 **Speaker 1** 30:58  
That's on competitive risk.

31:00  
Competitive risk.

 **Speaker 1** 31:00  
I don't think from a technology point of view there's much we can do there, I mean.  
I saw we had the presentation last week from.

31:11  
Medical underwriting.  
It's ultimately.

 **Speaker 1** 31:17  
Yeah, she did a presentation.

 **Vizzini, (Alain)** 31:18  
Yes.

31:19  
Yeah, yeah.

 **Speaker 1** 31:20  
So medical underwriting should do.  
The presentation looks very good, went from 5 days to six days down to one hour.  
Perfect, I said.  
Well, this is great.  
So are we the first in the industry?  
Were we the other ones to do it?  
And she said no, we're the last.  
Everybody else has done this for me.

31:34  
I was like.  
So.

 **Speaker 1** 31:38  
I'm. I'm not so worried about us taking on innovation, technology, innovation.  
I'm more worried about our business's ability to innovate quickly because I have been in meetings where the first thing we say we want to try something.  
I get question thrown back to me.  
We need to check what their competitors are doing.  
We need to see.  
We've got to stop this.  
You just have to go forward and you know you want to be at the front of the wave, not right at the back.  
It sounds like we're right at the.

32:09  
Business process.

 **Speaker 1** 32:10  
So that's a challenge.  
How do we?  
Accelerate innovation in the business side.

32:18  
OK.

 **Speaker 1** 32:19  
Anything else on innovation?  
Anybody wants to talk about?

32:23  
Gente Ki.

 **Speaker 1** 32:24  
Yeah, that's what I was gonna say.

 **Speaker 2** 32:25  
Well, maybe if you get a chance to.  
Yeah, I like to, you know, do the thinking for you and the business doesn't have to think anymore.

32:30  
Yeah. Well, we.

 **Speaker 1** 32:31  
I mean, we just, we just had a presentation from a vendor and they said that they could build something from scratch in Hiroshi challenge and said, OK, show me how to do it.  
So we, where'd you put it?  
Build us a MDM for Japan.

32:44  
Yeah.  
And it's.

 **Speaker 1** 32:49  
Really, it's the ghost.  
Does the whole SDLC process itself within the tool so built a system requirements and then goes through and does all the the testing sets up all the tests to it? Then it comes up with basically builds the code for it. We we saw at the end of list.  
Of Jason file that can start to generate the code, so it was.

33:08  
A start.

 **Speaker 1** 33:08  
It's a startupation up there.  
OK, sorry. I'll keep talking throughout.  
Keep going next. Then we'll.

 **Koide, (Kayo)** 33:18  
On Kenya team.

 **Speaker 1** 33:18  
I'd love to do with your risk, OK?  
Yeah. So this one Nagayoshi saw, so the.

 **Nagayoshi, (Takayuki)** 33:29  
I.

 **Speaker 1** 33:29  
Disaster recovery. I know that there's been some testing being done by Shibata San. Did first round of vendor testing last month.

 **Nagayoshi, (Takayuki)** 33:34  
Yes.

 **Speaker 1** 33:36  
We're going to Bender testing this month.  
All in preparation for doing the swing to doctor and run on the KKBC by 400 in November so.  
It seems like we're actually moving in the right direction here.

 **Nagayoshi, (Takayuki)** 33:51  
Hi.

 **Speaker 1** 33:54  
We haven't reduced the risk yet, but we're definitely moving in the right direction.

 **Nagayoshi, (Takayuki)** 33:58  
Yes. And we are going to, the is going to update the status in the next REMC meeting this week, yeah.

34:09  
This Friday, right? Yeah.

 **Nagayoshi, (Takayuki)** 34:12  
And currently the it's in, it's ongoing in progress with without any issue at present. Of course some some minor technical challenges exist, but overall is OK.  
I.

 **Speaker 1** 34:32  
Business continuity. I feel like we've got we're in a much better position now.  
Than two months ago, we did the delta wall.  
Drill you know PDB and Yep, with Eric, they're taking charge.

34:44  
Peter.

 **Speaker 1** 34:47  
And as it should be BCM taking the lead and as you said here you noted that some business colleagues did not take BCP seriously.

34:56  
They're getting a.

 **Speaker 1** 34:56  
Little bit more serious about it. Still, there's some that are a little bit more.  
I think it's we're in a better position now than we were, especially in terms of customer leak and compliance sales and and you know everybody except for our.  
Technology understanding their.

35:15  
Call.

 **Speaker 1** 35:15  
Sudo, but now I think we still.  
Need to keep.

35:18  
Improving.

 **Speaker 4** 35:18  
Yeah. Improvement momentum. Yeah.

 **Speaker 1** 35:20  
We we got a nice report from PwC that presented to Herman and I last Thursday, 102 pages still work to to beat up.

35:25  
Yeah.

 **Speaker 4** 35:29  
I think that's the way we feel like submitted to the RMC.  
The next one.

 **Speaker 1** 35:34  
To presented that, yeah.

35:37  
But.

 **Speaker 2** 35:38  
But then we just said business continuity.  
Do we want to put that under IT?

 **Speaker 1** 35:44  
Well, this was just more. We were just talking about the risks we see.  
So and this is more about just a general discussion we see as as a group about the risk of that. And so for me, I mean this is not something we need to do this.  
BCP BCM needs to take care of this is more that we see that as a risk and we should be talking about that without certificates doesn't just because it's on here doesn't mean we need to do it.

36:02  
OK.

 **Speaker 1** 36:06  
It's more that we use the general risk, OK.  
So when I ride in the ECF I can say hey, I see this is risky when I'm engaging in the ECF review, I can say Herman, you suck.  
So customer, you're BCP sucks.

36:19  
Or something. OK, cool. Thanks.

 **Speaker 4** 36:20  
So you are the owner for this, like continuity, risk control now, right?

 **Speaker 1** 36:25  
It is here, yeah.

36:25  
Yeah.

 **Speaker 4** 36:26  
So like you're right.

36:26  
Yes.

 **Speaker 1** 36:27  
Well, well, yeah.

36:28  
Oh.

 **Speaker 4** 36:29  
Well, definitely, yeah, that's yeah.  
Yes. Yeah, I think we like huge, yeah.

 **Speaker 1** 36:37  
Impact of this approval?  
Yeah. Well, two months ago we had a business improvement order. Now we don't, so.  
Job done, right?

36:44  
Yeah, maybe.

 **Speaker 4** 36:45  
Maybe that is like more to like operational change risk rather than less continuity.  
It's about like that.

36:51  
The resource.

 **Speaker 4** 36:51  
Maybe, you know, posed to this a bio that's kind of hindered the the business initiatives.  
So you may want to mention the bit about this if you want to in the report. Maybe under the personal chamber risk could be the data category.

 **Speaker 1** 37:07  
Yeah, but this was based on conversation last time where Michael was saying that we because of the bio, we shelved some of our plans for business continuity.

 **Speaker 4** 37:17  
So that that's where it is. OK, so the the actual impact was happening to this, OK.

 **Speaker 1** 37:23  
Yes, it is a risk.

 **Speaker 4** 37:24  
It is a.  
OK, but it's resolved then.  
Yeah, yeah. Cool.

37:30  
OK.

 **Speaker 1** 37:31  
Then I guess more broadly, does anybody see any?  
We had the general questions here and digital sovereignty, which that was quite funny.  
You know, this has a lot to do with Trump and other things as well.  
And then, yeah, so the reshoring offshoring is to do with trout.

37:55  
OK.

 **Speaker 1** 37:56  
Any other general?  
Risks we see.

38:00  
This time.

 **Speaker 1** 38:02  
You know, cross any of these?

 **Speaker 2** 38:04  
Just maybe third party.

 **Speaker 1** 38:05  
Yeah, third party risk is definitely increasing, yeah.  
Yeah. So we've seen nothing but.  
Problems locally in Japan with our specific vendors, but also globally with third party vendors as well, right?

 **Speaker 2** 38:18  
Yeah. And especially for Japan.  
Do not know it would.  
I would say in the more in the geopolitical is you know Japan is being hit hard and that's why the FSA has got a lot of problems on their hand.  
And it might be in, you know, as I said a little bit earlier, more they can probably more stricter.

38:36  
Yeah, with.

 **Speaker 2** 38:36  
A lot of their, you know, security say, hey, get it done, get it done.  
That means we have to make sure that a lot of the initiatives within the the security controls, yeah, have to be implemented in an earlier stage. Yeah. And something that we would think that we need to do maybe 2-3 years download that would be something so it.

 **Speaker 1** 38:53  
More about having capacity to implement that and it's not just capacity in the in the security team, but capacity in the teams that are built using those tools that they actually tools.

39:01  
Right or what?

 **Speaker 1** 39:01  
Implement MFA on my page or whatever it.

 **Speaker 2** 39:04  
Is and.

39:04  
But also.

 **Speaker 2** 39:05  
And then and then but.  
It will affect the business and yeah, our agents or things like that and that means you have to also talk to them.

39:11  
Yeah, sure.

 **Speaker 2** 39:11  
It's not just an IT issue. It's a company wide that needs to be driven to get to that or else some people are not going to be happy, you know.  
But it's the FSA is saying.  
We got to do it, but we have to make sure we say it in to make sure that the people who use it at the end understand that.

39:26  
Yeah, yeah.

 **Speaker 1** 39:27  
And I think, well, I mean, Aaron, this is part of the OKRs, right?  
0 is a regulatory and mandatory change.  
2 is business growth and three is is future ready so.  
01/2 yeah, go right at the bio now.

39:44  
So yeah.  
OK.

 **Speaker 1** 39:49  
That's fair enough.  
Again, it's going to come down to resources.  
This is what optimization is critical.  
OK, follow up tasks.  
Now we get in follow up tasks.  
Who set people up some context?  
OK. Confidential risk management, Aaron. Tata governance, build data dictionaries. Clean up necessary data. I think that's the calibra and the work that you're doing, which is good.  
Data loss protection. Yep.  
System scaling network with OK.  
So at least we know that those conversations are ongoing, but it does seem that.  
Group has not invested heavily in that team.  
Alright, there's only like one or two people, Renee or.

 **Speaker 2** 40:32  
Just Renee. And there's some other people. But I think only Renee's got the well. There's like 3 people who actually have the permission to do it.  
Yeah, but they don't do it.  
There's only Renee, who's actually does the actual changes right now.  
Yes, probably because of the resource constraints as she just said.

40:47  
OK, OK.

 **Speaker 1** 40:49  
Confederate information create a link and.  
Send this out.

40:55  
I.

 **Speaker 1** 40:55  
Think that sounds like the one for Salesforce, right?  
The Salesforce process.

 **Tsutsumi, (Hideaki)** 40:59  
Yes, but the issue that this sentence is a more general one because I I'm engaged in the only for the new product project of new product related information for the product project delivery but this sentence.  
Seems more broader, including new productive.

41:18  
It does.

 **Speaker 1** 41:18  
It's very broad, yes.

 **Tsutsumi, (Hideaki)** 41:21  
I.

 **Speaker 1** 41:22  
But again, this is the AI so.  
And I think it's linked to the one above it as well.  
Around the protection piece with.

41:30  
No.

 **Speaker 1** 41:33  
So I think that that can be fine. So I don't mind this one. You can put this more specifically to.  
Sells the new product confidential information.

 **Tsutsumi, (Hideaki)** 41:45  
E.

 **Speaker 1** 41:48  
Operational change when the funding centers are processed for operational changes, including requirements, UAT, sign off. OK. Yep, perfect.  
This one we're doing. Simly sign. You've got the deck.

 **Tsutsumi, (Hideaki)** 41:56  
Yeah, yeah, yeah, yeah.

 **Speaker 1** 41:57  
Yep, Aaron, it's more of this. One is more also then we just need to take that and put it into all projects, not just the product project 1, you know business requirements, ownership.

 **Ward, (Aaron Samuel)** 42:05  
Yeah, yeah. And and and and Khoi Desan and and and Yasmoltosan are working with with the border team on on on this. So the plans are in place to for doing this.

 **Speaker 1** 42:15  
Yeah, cabinar processes too fantastic.  
Good job :).  
Inspection of offshore teams. OK, tomorrow tomorrow will be in Vietnam. So enjoy.

42:30  
No.

 **Speaker 1** 42:33  
It might be cooler there than I mean, it can't be possibly be hotter than Tokyo so.  
Should be cruel.

 **Vizzini, (Alain)** 42:39  
Please don't go and jinx us. Thank you.

 **Speaker 1** 42:41  
Sorry, sorry, did I didn't mean to.

 **Speaker 2** 42:45  
I think the high was 35.

 **Speaker 1** 42:48  
Singapore was a lot cooler two weeks ago, right? So yeah.

42:53  
4/2.

 **Speaker 2** 42:53  
40 in Tokyo then yes.

 **Speaker 1** 42:55  
Yeah. Well, it's supposed to be 40.  
I think it's.

42:56  
Wednesday.

 **Speaker 1** 42:57  
Right.  
Yeah. God, that sucks.  
Uh ransomware prevention. Hence, for any way to spread ransomware texture or something, I think it's some way we have the ongoing stuff.  
It sounds like matus's done a great job, but it sounds like.

 **Speaker 2** 43:10  
But it's setting.  
The thickest 1 here is about the security awareness where NN Group has raised uh has released a solution for all of NN Group, right?  
So that you know the quarterly uh security awareness that comes from buzzword.

43:23  
Yup.

 **Speaker 2** 43:24  
That's a big one because it's the whole company.

43:27  
Yeah, you.

 **Speaker 2** 43:27  
Know it shows you that we're not doing just, you know, a little bit.  
You know, how would you say a newsletter or anything?  
No, it's something that we and it's being monitored, you get the numbers at the end, but you can see you know.

43:38  
On it.

 **Speaker 2** 43:39  
And if you need to chase, well, still the chase environment where I'm working on it. Yeah, but it's a company wide, you know initiative. So it shows you how important is.  
Yeah, but also on top of that, we still do the, you know, like the town hall or, you know, there was I think the one in alanzier.  
I don't know.  
We do there.  
Here and there and also the the newsletters in on the board basis.

44:00  
Of course.

 **Speaker 2** 44:01  
And then when it comes to October, we'll have to make sure that because it's cyber month and we'll do the newsletters on a weekly basis. But things of that nature we do, yeah, OK, good.

 **Speaker 1** 44:10  
And then lastly, legacy system risk, OK, I think, yeah, we we definitely have.  
A plan for life J, and now we just need a trigger and everybody else to get off Java, right?  
So that's also something for me to just work our way through over the next 12 months.  
Good, OK, kui dassad.  
Anything else we need to do for the process?

44:33  
So.

 **Koide, (Kayo)** 44:35  
We build to input up for the meeting result, but.

44:46  
There's a app.

 **Koide, (Kayo)** 44:46  
Sorry, it is again.

 **Speaker 1** 44:47  
Is it in the UDA list?

44:51  
You.

 **Koide, (Kayo)** 44:51  
You.

44:52  
Sky.

 **Koide, (Kayo)** 44:54  
As a public you created, but I noticed though it is very difficult to follow up tasks based on this this style is easier to talk.

 **Speaker 1** 44:54  
Who built this?

44:56  
What?  
Hmm.  
Yeah, but.

 **Speaker 1** 45:14  
OK, This is why.

 **Speaker 4** 45:15  
This is.  
Who created this?

 **Koide, (Kayo)** 45:16  
So.

 **Speaker 1** 45:17  
So there is an app.  
This is Herman.  
Know he has this app.

 **Koide, (Kayo)** 45:20  
At this Friday, it's Jia Sang and I will introduce this to him. The reason of this is the originally I all created the very long.

45:33  
Hmm.

 **Koide, (Kayo)** 45:36  
Long SharePoint, SharePoint mistakes. So it very difficult to input that and very difficult to follow up. So we decided to build up but.

45:37  
Excel sheet.

 **Speaker 1** 45:39  
A SharePoint, OK yeah.

45:47  
OK.

 **Koide, (Kayo)** 45:53  
So I'm not too easy to talk.

 **Speaker 1** 45:57  
Yeah, so so you can put like the second meeting date you put in today. And then if we want to update the content, you'll need to go in and manually update the content for each one, so.

 **Koide, (Kayo)** 45:58  
I.  
So, so, so, so, so, so. Basically just copy and paste from the Word document. So you can also see actions under the list.

46:13  
Yeah.  
Yeah.

 **Koide, (Kayo)** 46:22  
Demo.

46:24  
Yeah. OK.

 **Speaker 1** 46:25  
That's quite a heavy, yeah.

 **Speaker 4** 46:28  
Maybe a little suggestion like this is like stopping at the level 1 taxonomy, but under the level 1 for instance IT risk you have like 6 underlining like taxonomy level 2.  
So if you can like break them down into those categories and then just mapping those, the the risks you discuss.  
Under those six categories, it'll be more like simpler.  
Wow for example, like you talk about third party and other it risk.  
They do. One such. What was that?

47:01  
I.

 **Speaker 4** 47:01  
Business partner risk. So like I'm the business partner risk we focus on, we see the risks there and then we have this action ongoing something like this. So it can be a bit more like structure instead of like a very descriptive role.

 **Koide, (Kayo)** 47:16  
Mm.

47:17  
You know, yeah.  
OK.  
Yeah.

 **Speaker 1** 47:20  
Yeah. I mean, I think the the, the, the outcome I want is that people are more aware of the risks, right? If we go OK, we're going through what is it 5 high level first level risk now and if that means we need to go through, I Don.

47:25  
Yeah, yeah.  
Yeah, yeah.  
Yeah.

 **Speaker 1** 47:35  
Know 22nd level risks.

 **Speaker 4** 47:38  
Yeah, but yeah.

 **Speaker 1** 47:39  
Is it just becoming process or process sake or are we actually getting the outcome we want which is the people aware of the risks as a group in technology?

47:45  
Yeah.

 **Speaker 1** 47:47  
Yeah. So I need to find a balance here.

 **Speaker 4** 47:50  
Yeah, I don't want to make it too complicated, but I could.  
The granularity of the risk you discuss here looks quite good.  
Just so you just put in the labeling. Yeah. Yeah. As like, this is about, like IT change risk. This is about like a so.

 **Speaker 1** 48:05  
OK, OK. So if you label OK about the high level in this paper application?

48:09  
Yeah, exactly.

 **Speaker 4** 48:11  
Exactly so that like you can like easily map those.  
Agenda under some risks, yeah.  
And then you don't necessarily need to describe everything.  
Copy and paste from there to here, but at least you can highlight some of the important things.  
Yeah. And derma and.

 **Speaker 1** 48:30  
OK. Because, I mean, \*\*\*\*\* wants to run this out for every area, right? So.

 **Speaker 4** 48:33  
Yeah, yeah, yeah.  
And by the way, the group is more focusing on to like every risk falling into the level 2 and this is what we have to make sure going forward.

 **Koide, (Kayo)** 48:36  
So.

48:43  
OK.

 **Speaker 1** 48:43  
So maybe a query sign if you want to try based on once you get the copilot summary of this meeting.  
Try to summarize.  
You know each section into the level 2 risk like the comments.  
See if you can tag it in the level 2 risk.  
Just tell me how easy or challenging that was.

49:03  
Yeah.

 **Koide, (Kayo)** 49:03  
Mm mm.

 **Speaker 1** 49:04  
Yeah. And then let's see.  
So and then when you present this with.

49:06  
Yeah.

 **Koide, (Kayo)** 49:06  
OK.

 **Speaker 1** 49:09  
Chia San to Herman on Friday.  
Yeah. So talk to him about that.

49:11  
Yeah, yeah.  
I see.

 **Speaker 1** 49:13  
Yeah, what he wants to.

 **Speaker 4** 49:14  
Do as well as you as a like a first. You can like already suggest some improvements.

49:19  
Right.  
Yeah, yeah.

 **Koide, (Kayo)** 49:22  
So this is a pattern. We have two patterns. This is at the quota meeting risk and this one is starting from this this quota discussion.

49:36  
Yeah, yeah.

 **Koide, (Kayo)** 49:37  
I.

 **Speaker 1** 49:40  
OK, send me the link because I need to think about this and we've got 5 minutes to talk about one other thing. So yeah.

 **Koide, (Kayo)** 49:45  
I.  
M.

 **Speaker 1** 49:49  
So I think we did discuss. Yeah, I think we did discuss it, OK.

 **Koide, (Kayo)** 49:54  
Right.

49:54  
Yeah. OK.  
OK, good.  
Thank you very much.

 **Speaker 1** 49:57  
Thank you Kui san.

 **Koide, (Kayo)** 49:59  
Hey, thank you. I.

50:00  
Thank you.

 **Ward, (Aaron Samuel)** 50:01  
Thank you.

 **Speaker 2** 50:01  
But he should talk about that.  
Will be of help.  
But if you're not gonna.

 **Speaker 1** 50:05  
Skip it then. Yeah, I think we'll skip that.  
To some of those, OK, so that we still has her camera on so.

50:18  
Yeah.

 **Speaker 1** 50:25  
Anyway, OK, OK.  
Thank you for that. That was.

50:30  
The.

 **Speaker 1** 50:32  
I think in the end valuable bit of a train wreck at the start, but we got there.  
Yeah, but it's only.  
It's only Round 2, so imagine how we do this in 10 years. Will be fine.

50:42  
What else?

 **Speaker 1** 50:43  
The only other thing so you guys are gonna be out for this week.  
Only Sitsumi San and Hiroshi and I will be here. I think everybody will be back next Tuesday, right?  
Yes, yeah, yeah. OK, good.

 **Ward, (Aaron Samuel)** 50:56  
Yep.

 **Speaker 1** 51:02  
One thing is I got a request.  
From remember I said to you a while back for CTO Mt.  
We have our dinners.  
He wants his him and his Mt want to come and join us.  
So maybe the August 28th 1, the last Thursday in August.  
Is see if they join us together, so I'll send an e-mail about that. He's checking with his guys now.  
I was thinking about doing it at the meijing beer garden.  
There's a beer garden there, a barbecue and beer.  
I think it's somewhere like ¥7000 or something, but it might be something good, yeah.

 **Tsutsumi, (Hideaki)** 51:41  
Um.  
Very hot.

51:46  
Well.

 **Speaker 1** 51:47  
We got a we got a sweat once, right?  
Feel, feel the warmth of big garden room, all that sort of stuff. So.

 **Ward, (Aaron Samuel)** 51:53  
Colby is OK.

 **Tsutsumi, (Hideaki)** 51:53  
Yeah.

 **Speaker 1** 51:55  
As long as it's not warm.

 **Tsutsumi, (Hideaki)** 51:56  
Oh.

 **Speaker 1** 51:58  
As long as it's not warm. Yeah, you can put ice in it. It'll be fine.

 **Speaker 2** 52:01  
Oh, is that gonna be over 100 days? No, no, September.

52:04  
It's OK.

 **Speaker 1** 52:05  
I can make all free and enjoy the show, so it's good.  
So that's it.  
Anybody taking obam?  
I think since I'm you're off for Obon, right?

 **Tsutsumi, (Hideaki)** 52:15  
Yeah, next week, yeah.

 **Speaker 1** 52:18  
Yeah, everybody else is working through.

 **Speaker 2** 52:21  
Yeah. Yeah. OK.

52:23  
2 minutes.

 **Speaker 1** 52:24  
Anything else anybody wants to raise?  
Speak now or forever hold your peace if we're good.

52:32  
Good. OK.

 **Ward, (Aaron Samuel)** 52:33  
All good.

 **Speaker 1** 52:33  
Have a safe trip, gentlemen.

 **Vizzini, (Alain)** 52:35  
Yeah.

 **Speaker 1** 52:36  
Watch out for Pierre and you know.

 **Vizzini, (Alain)** 52:38  
But you're the certain person saying that. Seriously, that's that's very scary.

 **Speaker 1** 52:44  
I've been there with him and it's it's an experience Ken has been.  
He's had the full Pierre twice so.

 **Vizzini, (Alain)** 52:49  
He was the first one talking to me about it.

52:53  
Yeah, yeah.  
So it's good.

 **Speaker 1** 52:53  
That's.  
OK, safe travels.  
Have a good time and I'll see you all.  
Yeah, next week.

 **Vizzini, (Alain)** 53:01  
Yeah, Aaron, see you in the airport tomorrow.

 **Ward, (Aaron Samuel)** 53:03  
Yep, cheers.

 **Vizzini, (Alain)** 53:04  
Yes, ma'am.

 **Koide, (Kayo)** stopped transcription